UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/662,811	09/16/2003	Hendrik Gerlach	1454.1501	1111

21171 7590 03/26/2007

STAAS & HALSEY LLP
SUITE 700
1201 NEW YORK AVENUE, N.W.
WASHINGTON, DC 20005

EXAMINER	
CHAI, LONGBIT	
ART UNIT	PAPER NUMBER
2131	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	03/26/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/662,811	GERLACH ET AL.	
	Examiner	Art Unit	
	Longbit Chai	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *29 January 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-29* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-29* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *16 September 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Priority

1. Applicant's claim for benefit of foreign priority under 35 U.S.C. 119 (a) – (d) is acknowledged.

The application is filed on 9/16/2003 but has a foreign priority application filed on 9/16/2002.

Claim Objections

2. Claims 1 and 25 are objected to because of the following informalities: "the outside of the appliance" and "the inside of the appliance" should be "an outside of the appliance" and "an inside of the appliance". Appropriate correction is required.

3. Claim 10 is objected to because of the following informalities: "the the security status" should be "the security status". Appropriate correction is required.

4. Claim 13 is objected to because of the following informalities: "A method ... comprising:" should be "A method ... comprising the steps of:". Appropriate correction is required.

5. Claim 20 is objected to because of the following informalities: "The method as claimed in wherein" should be, for example, "The method as claimed in claim 18, wherein". Appropriate correction is required.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraph of 35 U.S.C. 102 that forms the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. Claims 1 – 4, 6 – 9, 11 – 16, 18 – 21, 23 – 27 and 29 are rejected under 35 U.S.C. 102(e) as being anticipated by Black et al. (U.S. Patent 2003/0041264).

As per claim 1, Black teaches a system comprising:

an appliance-internal unit to detect a security status of an appliance (Black: Para [0006] Line 1 – 3, Para [0036] and Para [0025]);

an external display to display the security status of the appliance directly on the outside of the appliance (Black: Para [0050] Line 14 – 16: the security status is externally displayed to a user or an administrator);

an internal display to display the security status of the appliance within the inside of the appliance (Black: Para [0010] Line 1 – 6: the internal event log identified as a format of (SRC, TARGET, CLASS) is considered as an internal display – This is also consistent with the specification of the instant application specification that states "the internal display" may be a simple mechanism such as the setting of a flag (SPEC: Para [0024] last two sentences)); and

a transmission unit to transmit security status data between other appliances in a network of appliances such that the security status data can be subjected to data processing in the network of appliances (Black: Para [0035] – [0036] and Para [0050]: each event of a computer is transmitted over the network and correlated / grouped as a network event).

As per claim 13, Black teaches a method for display and detection of a security status of an appliance comprising:

detecting the security status of the appliance (Black: Para [0006] Line 1 – 3, Para [0036] and Para [0025]);

displaying the security status of the appliance on an outside of the appliance (Black: Para [0050] Line 14 – 16: the security status is externally displayed to a user or an administrator);

displaying the security status of the appliance on an inside of the appliance (Black: Para [0010] Line 1 – 6: the internal event log identified as a format of (SRC, TARGET, CLASS) is considered as an internal display – This is also consistent with the specification of the instant application specification that states "the internal display" may be a simple mechanism such as the setting of a flag (SPEC: Para [0024] last two sentences); and

transmitting data between appliances in a network of appliances such that security status data can be subjected to data processing in the network of appliances

(Black: Para [0035] – [0036] and Para [0050]: each event of a computer is transmitted over the network and correlated / grouped as a network event).

As per claim 25, Black teaches a automation appliance for display of a security status, having:

an appliance-internal unit to detect the security status of the appliance (Black: Para [0006] Line 1 – 3, Para [0036] and Para [0025]);

an external display to display the security status of the appliance directly on the outside of the appliance (Black: Para [0050] Line 14 – 16: the security status is displayer to a user or an administrator); and

an internal display to display the security status within the inside of the appliance in a format readable by other internal devices within the appliance (Black: Para [0010] Line 1 – 6, Para [0035] and Para [0050] / [0048] & Figure 5: (a) the internal event log identified as a format of (SRC, TARGET, CLASS) is considered as an internal display – This is also consistent with the specification of the instant application specification that states "the internal display" may be a simple mechanism such as the setting of a flag (SPEC: Para [0024] last two sentences (b) i.e., a common format for a classified event group associated with a particular network situation that can be communicated within the network).

As per claim 2 and 14, Black teaches the appliances are automation appliances (Black: Para [0006] Line 7 – 10, Para [0009] and Para [0010]: automation user

programs is provided for the internal display as a common format event logs to prevent merely dumping the system events to an administrator to sort through and make sense of the data, as taught by Black).

As per claim 3, 15 and 26, Black teaches the external display visually displays the security status (Black: Para [0050] Line 14 – 16: the security status is displayer to a user or administrator).

As per claim 4, 16 and 27, Black teaches an access unit to run automation user programs on the internal display (Black: Para [0006] Line 7 – 10, Para [0010], Para [0009] and Para [0036]: (a) a computer access unit is provided for automation user programs for the internal display as a common format event logs to prevent merely dumping the system events to an administrator to sort through and make sense of the data, as taught by Black (b) the internal event log identified as a format of (SRC, TARGET, CLASS) is considered as an internal display – This is also consistent with the specification of the instant application specification that states "the internal display" may be a simple mechanism such as the setting of a flag (SPEC: Para [0024] last two sentences)

As per claim 6 and 18, Black teaches a joint display to display an overall security status of a plurality of appliances, respectively having their internal displays linked (Black: Figure 7 & 8, Para [0035] and [0050] / [0048] : the collection and correlation of

event logs from each computers within the network as a group network event is considered as a joint display).

As per claim 7 and 19, Black teaches the joint display is an external visual display (Black: Para [0050] Line 14 – 16: the correlated security status is displayer to a user or administrator).

As per claim 8 and 20, Black teaches there are a plurality of joint displays, each displaying the status of a different plurality of appliances (Black: Para [0036], Figure 4B / 4C, Figure 7 & 8, Para [0035] and Para [0050]), and the overall security status is passed on from the joint display to a higher-level joint display that displays an overall security status of the appliances communicating with the joint displays (Black: e.g., Figure 8, Table 1 and Para [0050]: Figure 8 / Element 802 is one type of joint display that is further passed on to a higher-level joint display of Figure 8 / Element 800).

As per claim 9 and 21, Black teaches there are a plurality of joint displays, each displaying the status of a different plurality of appliances (Black: Para [0036], Figure 4B / 4C, Figure 7 & 8, Para [0035] and Para [0050]), and a server is provided for administration and display of the respective status of the joint displays appliances (Black: Para [0025], Para [0035] and Figure 8 / Element 800).

As per claim 11 and 23, Black teaches a portion of the appliances have internal security mechanisms (Black: Para [0010], Para [0035] and Para [0050] & Figure 5: the internal event log identified as a format of (SRC, TARGET, CLASS) is considered as an internal security mechanisms – This is also consistent with the specification of the instant application specification that states "the internal display" may be a simple mechanism such as the setting of a flag (SPEC: Para [0024] last two sentences)), a portion of the appliances are without internal security mechanisms (Black: Para [0006] Line 7 – 10: "without internal security mechanisms" is considered as the method that merely dumps system events to an administrator to sort through and make sense of the data), and the system integrates appliances without internal security mechanisms with appliances that have internal security mechanisms (Black: Para [0010] and Para [0006] Line 7 – 10: a system can be managed with either automatically or manually as needed – This also appears in the application specification).

As per claim 12 and 24, Black teaches the transmission unit transmits security status via an Intranet and/or the Internet (Black: Para [0035]).

As per claim 29, Black teaches the internal display functions as an input for other devices within the appliance (Black: Para [0010], Para [0035] and Para [0050]: i.e., a common format for a classified event group associated with a particular network situation that can be communicated within the network).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 5, 17 and 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Black et al. (U.S. Patent 2003/0041264), in view of Grainger (U.S. Patent 6,910,135).

As per claim 5, 17 and 28, Black teaches collecting the event logs with a common format stored internally in the computer memory as an internal-information base, accessing to the security status being provided by the internal display and communicating each of computer events over the TCP/IP network that are correlated / grouped as a network event (Black: Para [0010], Para [0035] – [0036], Page 2 / Left Column / Line 1 – 5 and [0050] / [0048]).

However, Black does not disclose expressly an internal-information base to provide access to the security status from the network of appliances via standard protocols.

Grainger teaches an internal-information base to provide access to the security status from the network of appliances via standard protocols (Grainger: Column 3 Line

18 – 23 / Line 32 – 36: SNMP / MIB (Management Information base) is used by an event correlation engine as a common information base and standard protocol for managing network events such as security status).

Accordingly, Black in view of Grainger teaches an internal-information base to provide access to the security status from the network of appliances via standard protocols, access to the security status being provided by the internal display (See the reasons set forth above).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Grainger within the system of Black because (a) Black teaches detecting and presenting the network security and intrusion information relating to a series of security violations to a user by collecting the event logs with a common format stored internally in the computer memory as an internal-information base, accessing to the security status being provided by the internal display and communicating each of computer events over the TCP/IP network that are correlated / grouped as a network event (Black: Para [0010], Para [0035] – [0036], Page 2 / Left Column / Line 1 – 5 and [0050] / [0048] (Black: Para [0002]) and (b) Grainger teaches providing an effective use of SNMP / MIB (Management Information base) by an event correlation engine as a common information base and standard protocol for managing network events such as security status (Grainger: Column 3 Line 18 – 23 / Line 32 – 36).

8. Claims 10 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Black et al. (U.S. Patent 2003/0041264), in view of Douglas (U.S. Patent 2004/0049693).

As per claim 10 and 22, Black does not disclose expressly the security status of the internal display can be simulated such that the internal display is active even without the appliance-internal unit detecting the security status.

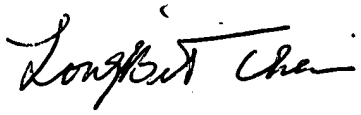
Douglas teaches the security status of the internal display can be simulated such that the internal display is active even without the appliance-internal unit detecting the security status (Douglas : Para [0089]: for debugging and testing purpose – This also appears in the application specification).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Douglas within the system of Black because (a) Black teaches detecting and presenting the network security and intrusion information relating to a series of security violations to a user (Black: Para [0002]) and (b) Douglas teaches host-based intrusion detection system (HIDS) that monitors, simulates, tests and debugs the system logs for evidence of malicious or suspicious application activity and detects attacks targeted at the host system on which it is installed and monitors output to the system and audit logs (Douglas : Abstract and Para [0089]).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 571-272-3788. The examiner can normally be reached on Monday-Friday 8:00am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.



Longbit Chai, Ph.D.
Patent Examiner
Art Unit 2131
3/19/2007